

# Smart Rewiring for Network Robustness

V. H. P. Louzada,<sup>1,\*</sup> F. Daolio,<sup>2</sup> H. J. Herrmann,<sup>1,3</sup> and M. Tomassini<sup>2</sup>

<sup>1</sup>*Computational Physics, IfB, ETH Zurich, Wolfgang-Pauli-Strasse 27, 8093 Zurich, Switzerland*

<sup>2</sup>*Faculty of Business and Economics, University of Lausanne, Lausanne, Switzerland*

<sup>3</sup>*Departamento de Física, Universidade Federal do Ceará, 60451-970 Fortaleza, Ceará, Brazil*

(Dated: March 22, 2013)

While new forms of attacks are developed every day to compromise essential infrastructures, service providers are also expected to develop strategies to mitigate the risk of extreme failures. In this context, tools of Network Science have been used to evaluate network robustness and propose resilient topologies against attacks. We present here a new rewiring method to modify the network topology improving its robustness, based on the evolution of the network largest component during a sequence of targeted attacks. In comparison to previous strategies, our method lowers by several orders of magnitude the computational effort necessary to improve robustness. Our rewiring also drives the formation of layers of nodes with similar degree while keeping a highly modular structure. This “modular onion-like structure” is a particular class of the onion-like structure previously described in the literature. We apply our rewiring strategy to an unweighted representation of the World Air Transportation network and show that an improvement of 30% in its overall robustness can be achieved through smart swaps of around 9% of its links.

## INTRODUCTION

The construction of a robust infrastructure network represents a great challenge to our society. In order to guarantee a broad and efficient coverage of basic services such as water, electricity, and telecommunications, decision makers need to take into account the effects of a great number of threats to the correct functioning of the system [1, 2]. Targeted terrorist attacks or random extreme weather conditions impose a systemic risk of catastrophic failure that has to be mitigated. In this way, tools provided by Network Science have offered interesting insights on common features of robust networks or methods and strategies to protect infrastructures [3–8].

Consider the construction of an air-transportation network as an example, a challenge currently faced by many developing nations [9, 10]. The localization of the airports should be decided given a tight supply and demand rule in order to ensure their efficiency, but other factors should also be included in the planning, such as security measures or noise reduction [11]. Besides that, the overall system robustness should be taken into account, as the transportation of goods and people cannot be entirely halted in case that some airports close.

When designing a new network from scratch, decision makers have an excellent opportunity to warrant its future robustness against failures [12]. However, most of the current infrastructure has been built in a non-supervised fashion, mostly through a preferential attachment mechanism, where highly connected nodes (e.g. airports, Internet Service Providers) have a higher probability of receiving a new link (e.g. flights, transmission cables) [13]. Inspired by this situation, we propose in this work a strategy to improve the robustness of a given network by a small number of interventions, which makes the method useful for real-time actions under budget con-

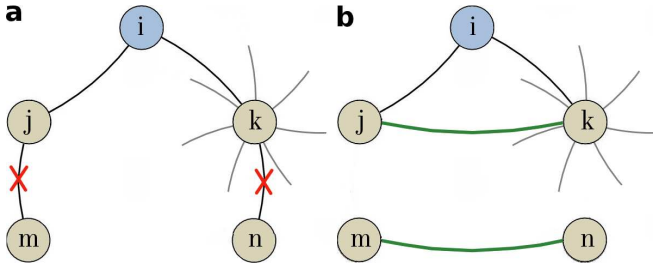
straints.

Simple modifications of the network topology, the connection pattern of nodes through links, have been shown to be an effective way to increase the robustness under node or link attacks [14–17]. In particular, Schneider et. al [18] showed that successive random rewirings (link swaps) create a robust network through the formation of an onion-like structure in which high-degree nodes compose a core with further interconnected layers of radially decreasing degrees.

In this work we propose a *smarter* rewiring that lowers by several orders of magnitude the computational effort necessary to improve robustness. Our method is consistently better than the random rewiring for a small number of swaps and yields the same level of robustness in the long term limit. An onion-like structure is also created, although a higher modularity and degree correlation is observed in comparison to networks created by random swaps. We apply our rewiring strategy to the World Air Transportation network and we show that an improvement of 30% in its overall robustness can be achieved through smart swaps of around 9% of its links.

## MODEL

In a Complex Network, nodes (representing power stations, airports, proteins, etc.) interact through links (cables, flights, molecular binding, etc.) resulting in complex behavior that describes technical and biological systems [19–25]. Particularly, Complex Networks provide significant insights into a system robustness, either in a static [26–29] or dynamic [30–35] context. We focus here on a generic approach to improve network robustness and consider only the simple case of networks where all links have the same importance (unweighted) and no



**FIG. 1. Smart Rewiring for robustness improvement.** Diagrammatic representation of the Smart Rewiring. **a**, First steps of the smart rewiring: For a randomly selected node ( $i$ , blue), its lowest degree neighbor ( $j$ , brown) and highest degree ( $k$ , brown) are selected. In sequence, two neighbors of  $j$  and  $k$  are randomly selected ( $m$  and  $n$ , both brown), and links to them ( $e_{jm}$  and  $e_{kn}$ ) are removed (red X). **b**, Last step of the smart rewiring in which links  $e_{jk}$  and  $e_{mn}$  (green) are added.

orientation (undirected). For illustration purposes, we explain our model and related concepts in the framework of the World Air-transportation Network, a system of paramount importance to our globalized world and that has been subject of a lot of research in the past years [36–38].

An Air-transportation network is defined here as *robust* when it allows a passenger to travel between most of the airports even considering the disruption of the service in the major connection hubs, i.e., the airports with largest number of flights. This feature is directly associated to the size of the largest connected component (LCC) of a network. In mathematical terms, robustness  $R$  is described as,

$$R = \frac{1}{N} \sum_{Q=1}^N s(Q), \quad (1)$$

where  $N$  is the number of nodes/airports,  $Q$  is the fraction of airports removed from the network, and  $s(Q)$  is the size of the LCC after the nodes were removed, considering that all incoming links/flights were also removed from the network. The parameter  $R$  is contained in the interval  $1/N \leq R < 1$ , and is a measure for robustness: a small  $R$  is associated to a fragile network and a larger  $R$  to a robust one.

To focus on targeted attacks, the node removal starts first with the highly connected nodes, the network hubs, which intuitively have the largest impact on the size of the LCC. After removing the more connected node we update the degrees (number of connections) of every node, and remove the next largest network hub. This process is further repeated until the network completely collapses.

To improve robustness, one could simply add more flights between airports. In the limit, the network becomes fully connected: one airport disruption does not affect other destinations. But improving an airport

flight capacity by adding redundancy might prove very impractical in the short term. In fact, numerous examples of infrastructure networks present this capacity constraint, such as adding new transmission lines to a power station or new traffic cables to an Internet Service Provider. Therefore, a rewiring strategy, where links are only swapped, keeping the nodes' degree fixed, is more appropriate: we reroute flights from airports and create new connection possibilities, without considerably changing the airports' load.

Here we propose a novel rewiring strategy that improves network robustness by creating alternative connections between parts of the network that would otherwise be split upon the failure of a hub. In our targeted attack scenario, we implicitly admit that the attacker perfectly knows the network degree sequence and thus can cause maximum damage. In the same way, we assume that the “defender” knows that the attacker has this information and thus acts upon it through a smart rewiring defined as follows:

1. Select a node  $i$  randomly with at least two neighbors with degree larger than one;
2. Select the lowest degree neighbor of  $i$ , the node  $j$ , and its highest degree neighbor, the node  $k$ ;
3. Select randomly a neighbor  $m$  of node  $j$  and a neighbor  $n$  of node  $k$ ;
4. Repeat steps 1-3 until all nodes concerned are different from each other.
5. Remove links  $e_{jm}$  and  $e_{kn}$ ;
6. Create links  $e_{jk}$  and  $e_{mn}$ .

where  $e_{ij}$  represents an undirected link between nodes  $i$  and  $j$ . An illustration of this strategy is provided in Fig. 1. At every step we compare the robustness  $R$  before and after the swap, and consider it a successful step if the robustness has improved. If unsuccessful, the swap is reverted and another smart rewiring is tested. In what follows,  $R_t$  represents the robustness after  $t$  steps are executed.

## RESULTS

A swap keeps the number of links and nodes' degree unchanged, and is capable of changing the network robustness. A simple example is presented in Fig. 2a-b for an unweighted representation of the World Air-Transportation Network. In this example, a single smart rewiring applied to an airport in Oceania is capable of improving the overall robustness by 1.85%. If a swap is randomly executed, however, there is no guarantee that an improvement occurs, or that the magnitude of the

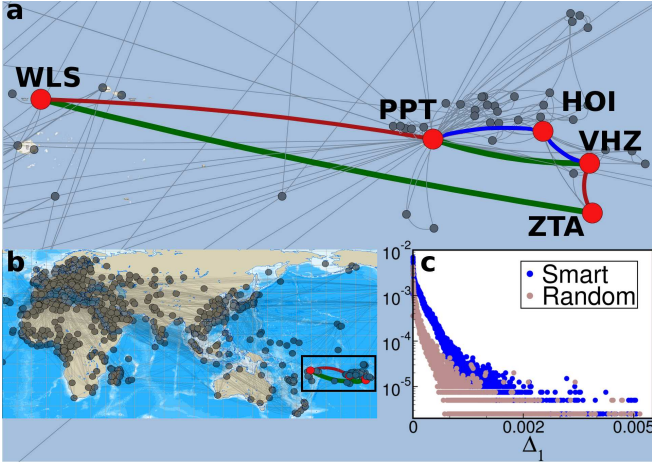


FIG. 2. **Proposed rerouting of flights for some airports in Oceania.** **a**, Example of the smart rewiring applied to the Hao Island Airport (HOI node), connected (in blue) to Faaa Airport (PPT), a regional hub, and to Vahitahi Airport (VHZ), a small airport. Connections Wallis Island (WLS) to Tureira Airport (ZTA) and PPT to VHZ are added (in green), while previous links from WLS to PPT and VHZ to ZTA are removed (in red). This simple swap increases the robustness of the World Air-Transportation unweighted network by 1.85%. **b**, Section of the World Transportation network showing the region in which airports in **a** are located. **c**, Effects of a single swap following the random and smart strategies on the overall robustness of a set of randomly generated Barabási-Albert networks.

improvement is satisfactory. Smart rewiring diminishes this problem as it presents a bias toward improvement. In a set of Barabási-Albert (BA) networks, the distribution of the robustness improvement after one swap,  $\Delta_1 = R_1 - R_0$ , shows that significant changes of robustness are more common with our strategy (Fig. 2c).

If positive swaps are executed in sequence, a systematic increase in the network robustness is achieved. Schneider et al. [18] showed an improvement of roughly 100% in  $R$  for a network of  $N = 1000$  after an extremely large number of swaps. Successive applications of the smart rewiring are much more efficient. We compare the evolution of  $R$  in both methods starting from a set of BA networks in Fig. 3, and while the smart rewiring doubles  $R$  after roughly  $10^6$  steps (positive or discarded swaps), random swaps are still at the level of 20% improvement. The collapse of the LCC happens after a removal of 52% of the nodes, a 50% improvement over the random rewiring strategy (Inset of Fig. 3). Tests for different network sizes show that the performance difference increases with network size (See Fig. S2 in Supplementary Material). In the limit of many swaps, both methods generate networks with the same level of robustness. Successive swaps in the World Air-transportation network improve its robustness by 4.82% with as few as 50 positive swaps, 0.32% of the total of links, as shown in Fig. 4a. In this network,

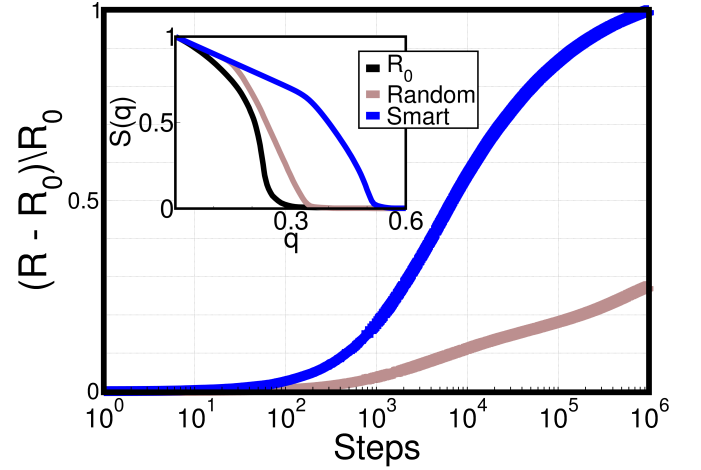


FIG. 3. **Fast Improvement of network robustness for the smart rewiring strategy.** The smart rewiring allows a much faster improvement of  $R$  in comparison to the random strategy. For  $10^6$  steps, the inset shows the LCC during a sequence of targeted attacks.

for a fixed level of robustness improvement (30%), smart swaps affect only  $9.24\% \pm 0.53\%$  of the total of links, while random swaps have to change  $15.19\% \pm 0.90\%$  links (Fig. 4b).

Successive applications of the smart rewiring change drastically another characteristics of the network as well. Fig. 4c shows the evolution of modularity [39] ( $Q$ ) during rewiring steps. The smart rewiring makes networks consistently more modular than random rewiring. This difference is a consequence of the intervention performed in the local connectivity by the smart rewiring, as our strategy deliberately creates triangles of connections. This structure reduces the importance of the hubs, which are now connected to leaves (nodes of low degree), and their removal does not have huge impact on global connectivity. These results are valid for different system sizes (See Fig. S2 in Supplementary Material).

Despite the creation of connections between hubs and leaves, network assortativity [40] *increases*, as the evolution of Newman's  $r$  coefficient shows in Fig. 4d. This result can be qualitatively understood considering the edges swapped. Before the rewiring, two edges contribute in a negative way to assortativity:  $e_{jm}$  connects a leaf to an average degree node and  $e_{kn}$  connects a hub to an average node. After the rewiring, one edge contributes negatively ( $e_{jk}$  connects leaf to hub) and the other contributes positively ( $e_{mn}$  connects average to average nodes). This effect is also persistent for different system sizes (See Fig. S2 in Supplementary Material) and considering assortativity through neighbor connectivity [41] (See Fig. S1 in Supplementary Material). In comparison, both the original BA networks and networks optimized through random swaps are disassortative.

Higher modularity and assortativity produced by the



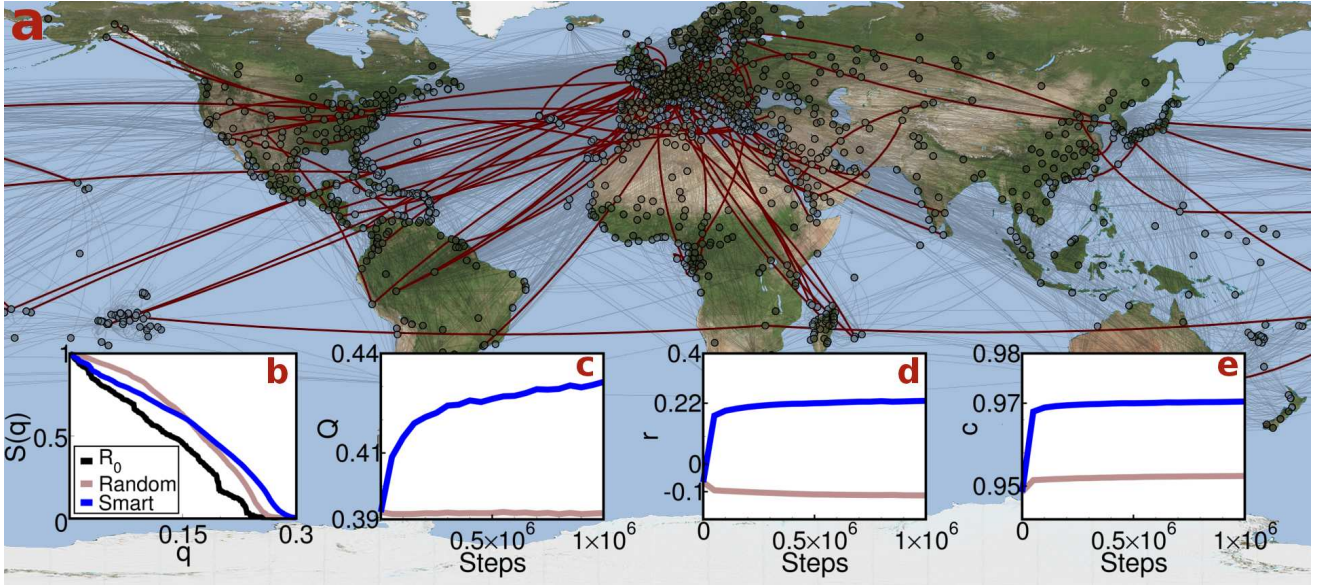


FIG. 4. **Robust Air transportation network.** **a**, The World Air Transportation Network has its robustness improved by 4.82% with swaps of 50 links (red) following the smart rewiring strategy. **b**, Size of the largest cluster for the World Air Transportation Network through a sequence of targeted attacks before and after the application of the smart and random rewiring strategies. In this case, both strategies reach the same level of robustness (30% of improvement), but while random rewiring changes  $15.19\% \pm 0.90\%$  of network links, smart rewiring changes only  $9.24\% \pm 0.53\%$ . **c-e**, Modularity ( $Q$ ), Assortativity ( $r$ ), and Onionlikeness ( $c$ ) during the application of the random and smart rewiring strategies.

smart rewiring do not interfere with the formation of the onion-like structure, where layers of nodes of increasing degree hold the network robustness. This structure can be quantified through an *Onionlikeness* parameter  $c$ ,  $1/k^* \leq c < 1$ , where  $k^*$  represents the highest network degree, for which  $c$  is positively correlated to the presence of an onion-like structure (more details given in the Supplementary Material). Both strategies produce the onion-like structure but, by yielding a larger robustness, the onion structure is more prominent in the case of the smart rewiring (Fig. 4e). Onionlikeness also remains larger for smart rewiring for different system sizes (See Fig. S2 in Supplementary material).

## DISCUSSION

Through a simple rewiring strategy we present here a method that improves drastically the network robustness while consuming little computational time. The proposed smart rewiring quickly increases robustness in comparison to a random choice of links. The high efficiency, together with the fact that only local knowledge of the two first neighbors of a given node is necessary, makes this strategy a potential tool for network designers and policy makers having the task of protecting our already built infrastructure against targeted attacks. As an example, simple interventions on the World Air Transportation Network have been able to considerably improve its

robustness. Our main analysis is performed on a set of randomly generated BA networks, which suggests that the same findings would apply to all real networks with a broad degree distribution function since the smart swap is general and not limited to a particular network class.

Besides its simplicity, the smart strategy counterintuitively improves the maintenance of the largest cluster through a local division of the network: at each step five nodes previously connected are transformed into a triangle and a pair of nodes. This apparent division does not fully fragment the network, it only reduces the importance of the network hubs in keeping the global connectivity through the addition of links between nodes of average degree. These rewired links might eventually bridge different parts of the network after the hub failure. Moreover, smart rewiring creates also a highly modular and assortative topology while forming an onion-like structure.

As modularity and assortativity differ radically from networks modified through random swaps, we define the structure of networks generated through successive applications of the smart rewiring as a *modular onion* structure. This new topology gives rise to the question if further changes in the swap mechanism could create different structures. Following this, swap mechanisms could be designed to improve a certain desired feature, in the same way as the smart rewiring enhances modularity, while improving network robustness. As a method based on a simplified framework, another possible application

of the current study is to adapt the strategy to real-time circumstances of an infrastructure network, such as flight capacity and climate conditions in the air transportation problem.

It is noteworthy that our model does not account for weights in the links, which would represent the number of passengers travelling between airports in a certain period of time. A rewiring method that takes advantage of this information, together with adaptations of the robustness concept, could have direct applications in the optimization of a real technical system.

## METHODS

The World Air Transportation Network was retrieved from Amiel et. al [37]. It contains data regarding only international airports and flights. The total amount of nodes/airports is 1326, with 16001 links, and average degree of 24.13. Artificial networks considered in this work are all BA networks of average degree six.

In Fig. 2, Panels **a** and **b** represent sections of the World Air Transportation. In particular, Panel **a** follows the IATA airport code at the labels. Panel **c** is an average over 100 BA networks of 1000 nodes, the standard deviation of the points being smaller than the symbols.

In Fig. 3, the main plot is an average over 100 BA networks of 2005 nodes. The inset is an average of 100 BA networks of 1000 nodes subjected to  $10^5$  steps of rewiring (Smart or Random) in comparison to the original network. In both plots the thickness of the lines is bigger than the standard deviation.

The main plot of Fig. 4 contains the entire World Air Transportation network with rewired links in red and thicker. The location of some airports are slightly altered due to map projection distortions. Inset **b** contains data regarding the Air network before and after  $10^5$  smart swaps, for which the smart rewiring curve is an average over 100 different sequences of random swaps. Insets **c-e** are averages over 100 BA networks of 2005 nodes. In all insets the thickness of the lines is bigger than the standard deviation.

**Acknowledgments.** Authors would like to thank the Swiss National Science Foundation under contract 200021 126853, the CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico - Brasil, the European Research Council under grant FP7-319968, and the ETH Zurich Risk Center for financial support. We would like also to thank N. A. M. Araújo and K. J. Schrenk for the valuable discussions.

- tolerance of complex networks. *Nature* **406**(6794), 378–382 (2000).
- [2] Helbing, D. *Systemic Risks in Society and Economics*. Paper prepared for IRGC Workshop on Emerging Risks, (2009).
- [3] Frank, H. and Frisch, I. T. Analysis and Design of Survivable Networks. *IEEE T Commun Techn* **18**, 501–519 (1970).
- [4] Molloy, M. and Reed, B. A critical point for random graphs with a given degree sequence. *Random Struct Algor* **6**, 161–179 (2000).
- [5] Paul, G., Tanizawa, T., Havlin, S., and Stanley, H. E. Optimization of robustness of complex networks. *Eur Phys J B* **38**, 187–191 (2004).
- [6] Ash, J. and Newth, D. Optimizing complex networks for resilience against cascading failure. *Physica A* **380**, 673–683 (2007).
- [7] Moreira, A., Andrade, J., Herrmann, H., and Indekau, J. How to Make a Fragile Network Robust and Vice Versa. *Phys Rev Lett* **102**, 018701 (2009).
- [8] Rokneddin, K., Ghosh, J., Dueñas-Osorio, L., and Padgett, J. E. Bridge retrofit prioritisation for ageing transportation networks subject to seismic hazards. *Struct Infrastruct E*, DOI:10.1080/15732479.2011.654230 (2012).
- [9] The Economist. *World in figures: Industries Infrastructure*, <http://www.economist.com/news/21566563-infrastructure>, accessed on 17th of December of 2012. (2012).
- [10] France 24. *Brazil announces construction of 800 airports*, <http://www.france24.com/en/20121212-brazil-announces-construction-800-airports>, accessed on 17th of December of 2012. (2012).
- [11] Swissinfo. *Compromise reached in Zurich airport row*, <http://swissinfo.ch/eng/i.html?cid=33027782&sb=twi>, accessed on 17th of December of 2012. (2012).
- [12] Havlin, S., Kenett, D. Y., Ben-Jacob, E., Bunde, A., Cohen, R., Hermann, H., Kantelhardt, J. W., Kertész, J., Kirkpatrick, S., Kurths, J., Portugali, J., and Solomon, S. Challenges in network science: Applications to infrastructures, climate, social systems and economics. *Eur Phys J-Spec Top* **214**, 273–293 (2012).
- [13] Barabási, A.-L. and Albert, R. Emergence of Scaling in Random Networks. *Science* **286**, 509–512 (1999).
- [14] Jiang, Z., Liang, M., and Guo, D. Enhancing Network Performance By Edge Addition. *Int J Mod Phys C* **22**, 1211–1226 (2011).
- [15] Zeng, A. and Liu, W. Enhancing network robustness against malicious attacks. *Phys Rev E* **85**, 066130 (2012).
- [16] Peixoto, T. P. and Bornholdt, S. Evolution of Robust Network Topologies: Emergence of Central Backbones. *Phys Rev Lett* **109**, 118703 (2012).
- [17] Wang, J. Robustness of complex networks with the local protection strategy against cascading failures. *Safety Sci* **53**, 219–225 (2013).
- [18] Schneider, C. M., Moreira, A. a., Andrade, J. S., Havlin, S., and Herrmann, H. J. Mitigation of malicious attacks on networks. *P Natl Acad Sci USA* **108**, 3838–3841 (2011).
- [19] Watts, D. J. *Small Worlds: The Dynamics of Networks Between Order and Randomness*. (Princeton Univ Press, Princeton), (1999).
- [20] Latora, V. and Marchiori, M. Efficient Behavior of Small-World Networks. *Phys Rev Lett* **87**, 198701, October (2001).

---

\* louzada@ethz.ch

[1] Albert, R., Jeong, H., and Barabasi, A. Error and attack

- [21] Maslov, S. and Sneppen, K. Specificity and stability in topology of protein networks. *Science* **296**, 910–913 (2002).
- [22] Dorogovtsev, S. N. and Mendes, J. F. F. *Evolution of Networks: From Biological Nets to the Internet and WWW*. (Oxford University Press, New York), (2003).
- [23] Newman, M. E. J. The Structure and Function of Complex Networks. *SIAM Review* **45**, 167–256 (2003).
- [24] Caldarelli, G. *Scale-Free Networks: Complex Webs in Nature and Technology (Oxford Finance)*. (Oxford University Press, New York), (2007).
- [25] Mamede, G. L., Araújo, N. A. M., Schneider, C. M., Araújo, J. C., and Herrmann, H. J. Overspill avalanching in a dense reservoir network. *Proc Nat Acad USA* **109**, 7191–7195 (2012).
- [26] Holme, P., Kim, B., Yoon, C., and Han, S. Attack vulnerability of complex networks. *Phys Rev E* **65**, 056109 (2002).
- [27] Albert, R., Albert, I., and Nakarado, G. Structural vulnerability of the North American power grid. *Phys Rev E* **69**, 025103 (2004).
- [28] Sydney, A., Scoglio, C., Youssef, M., and Schumm, P. Characterizing the Robustness of Complex Networks. *IJITST* **2**, 291–320 (2010).
- [29] Louzada, V. H. P., Daolio, F., Herrmann, H. J., and Tomassini, M. Generating Robust and Efficient Networks Under Targeted Attacks, on arXiv:1207.1291.
- [30] Boccaletti, S., Farini, A., and Arecchi, F. T. Adaptive synchronization of chaos for secure communication. *Phys Rev E* **55**, 4979 (1997).
- [31] Motter, A. and Lai, Y.-C. Cascade-based attacks on complex networks. *Phys Rev E* **66**, 065102(R) (2002).
- [32] Wang, X. F. and Chen, G. Synchronization in scale-free dynamical networks: robustness and fragility. *IEEE T Circuits-I* **49**, 54–62 (2002).
- [33] Raposo, E. P., Buldyrev, S. V., da Luz, M. G. E., Santos, M. C., Stanley, H. E., and Viswanathan, G. M. Dynamical Robustness of Lévy Search Strategies. *Phys Rev Lett* **91**, 240601 (2003).
- [34] Shargel, B., Sayama, H., Epstein, I., and Bar-Yam, Y. Optimization of Robustness and Connectivity in Complex Networks. *Phys Rev Lett* **90**, 068701 (2003).
- [35] Louzada, V. H. P., Araújo, N. A. M., Andrade, J. S., and Herrmann, H. J. How to suppress undesired synchronization. *Scientific reports* **2**, 658 (2012).
- [36] Guimerà, R., Mossa, S., Turtchi, A., and Amaral, L. A. N. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proc Nat Acad USA* **102**, 7794–7799 (2005).
- [37] Amiel, M., Mélançon, G., and Rozenblat, C. Réseaux multi-niveaux: l'exemple des échanges aériens mondiaux de passagers. *Mappemonde* **79**, 1–12 (2005).
- [38] Colizza, V., Barrat, A., Barthélemy, M., and Vespignani, A. The role of the airline transportation network in the prediction and predictability of global epidemics. *Proc Nat Acad USA* **103**, 2015–2020 (2006).
- [39] Blondel, V. D., Guillaume, J.-L., Lambiotte, R., and Lefebvre, E. Fast unfolding of communities in large networks. *J Stat Mech* **P10008** (2008).
- [40] Newman, M. E. J. Assortative Mixing in Networks. *Phys Rev Lett* **89**, 208701 (2002).
- [41] Pastor-satorras, R., Vaquez, A., and Vespignani, A. Dynamical and correlation properties of the Internet. *Phys Rev Lett* **87**, 258701 (2001).